



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/693,713	10/19/2000	Kunihiko Miyazaki	16869P-011500	7398

20350 7590 03/29/2006

TOWNSEND AND TOWNSEND AND CREW, LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA 94111-3834

EXAMINER

HOFFMAN, BRANDON S

ART UNIT PAPER NUMBER

2136

DATE MAILED: 03/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/693,713	MIYAZAKI ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 09 January 2006.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 39-52 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 39-52 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. Claims 39-52 are pending in this office action (all of which are newly added), claims 7, 9-12, 21, 23-26, 30, and 34-38 are canceled.
2. Applicant's arguments, filed January 9, 2006, with respect to the independent claims have been considered but are moot in view of the new ground(s) of rejection.

### ***Rejections***

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

### ***Claim Rejections - 35 USC § 112***

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:  

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.
5. Claim 41 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
6. Claim 41 recites the limitation "permitting registration." It is unclear what the applicant's intended metes and bounds for the claim is.

***Claim Rejections - 35 USC § 103***

7. Claims 39-52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier et al. (U.S. Patent No. 5,956,404) in view of Glass (U.S. Patent No. 6,553,494).

Regarding claims 39, 43, and 50, Schneier et al. teaches a digital signing method/apparatus/computer program product, comprising:

- A processor (col. 5, lines 22-28);
- A storage medium, wherein said processor computes a hash value of inputted data including a message to be signed or a hash value thereof (col. 6, lines 40-50 and fig. 4, ref. num 306), and wherein
- Said processor encodes the computed hash value of the inputted data into encoded data of a predetermined format that is suitable for encryption processing for generating a signature (col. 8, lines 10-17);
- Said processor applies a secret key to the encoded data to generate a digital signature for the message to be signed (col. 6, lines 50-52 and fig. 4, ref. num 308);
- Said processor prepares a signature-attached data including the message to be signed, and the previous log data or the hash value thereof for generating the signature (fig. 6); and
- Said processor registers log data of said signature-attached data with a log list in said storage medium (col. 11, lines 25-29).

Schneier et al. does not teach that the signature-attached message includes the digital signature for the message, the message, and the previous log data or hash value. Schneier et al. rather shows a message that includes the previous message or hash value, appended with the current message, and all of that is hashed. Schneier et al. falls short in that there is no digital signature attached to the appended message before hashing.

Glass teaches a signature-attached data including the digital signature for the message, the message, and previous data (col. 4, lines 26-39, 57-65, col. 5, line 57 through col. 6, line 6, and col. 10, lines 1-4).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a digital signature, message, and previous data all appended together, as taught by Glass, with the method/apparatus/computer program product of Schneier et al. It would have been obvious for such modifications because the binding performed in Glass provides for authentication of the chain of hashed documents.

Regarding claim 44, Schneier et al. as modified by Glass teaches wherein

- Said processor applies said secret key to a message or the hash value thereof to generate a digital signature for the message (see col. 6, lines 50-52 and fig. 4, ref. num 308 of Schneier et al.); and wherein

- Said processor prepares a signature-attached data that includes the generated digital signature, the message, and the previous log data or hash value thereof (see fig. 6 of Schneier et al. and col. 4, lines 26-39, 57-65, col. 5, line 57 through col. 6, line 6, and col. 10, lines 1-4 of Glass); and wherein
- Said processor registers log data of a signature-attached data include the generated digital signature, the message, and the previous log data or hash value thereof, with said log list (see col. 11, lines 25-29 of Schneier et al.).

Regarding claims 40 and 45, Schneier et al. as modified by Glass teaches wherein said log data further comprises a distribution destination (see col. 6, lines 27-29 of Schneier et al.).

Regarding claims 41 and 46, Schneier et al. as modified by Glass teaches wherein registration of the log data with said log list is permitted only when the previous log data is included in the latest log data registered with said log list (see col. 11, lines 45-48 of Schneier et al.).

Regarding claims 42 and 47, Schneier et al. as modified by Glass teaches wherein

- Said processor obtains a timestamp from a trusted authority, said timestamp generated by applying a second secret key to the digital signature, and a time (see col. 12, lines 41-48 of Schneier et al.); and

- Said processor prepares said signature-attached data including the generated digital signature, the message, and the previous log data or hash value thereof, and the timestamp (see fig. 6 of Schneier et al. and col. 4, lines 26-39, 57-65, col. 5, line 57 through col. 6, line 6, and col. 10, lines 1-4 of Glass).

Regarding claim 48, Schneier et al. as modified by Glass teaches further comprising an interface configured to be connectable to a computer (see fig. 1, ref. num 61 of Glass).

Regarding claim 49, Schneier et al. as modified by Glass teaches wherein

- If a number of the log data registered with the log list exceeds a particular value, said processor outputs at least one of a plurality of log data registered with the log list to said computer, whereupon said computer registers said at least one of a plurality of log data with a second log list prepared in said computer (see col. 12, lines 49-60 of Schneier et al.), and thereupon,
- Said processor deletes said at least one of a plurality of log data from said log list in said storage medium (see col. 12, lines 1-15 of Schneier et al.).

Regarding claim 51, Schneier et al. as modified by Glass teaches wherein the computer readable storage medium is a computer readable medium for storing the codes (see col. 3, lines 22-24 of Schneier et al.).

Regarding claim 52, Schneier et al. as modified by Glass teaches wherein the computer readable storage medium is a computer readable medium for transmitting the codes (see col. 8, lines 28-31 of Schneier et al.).

### ***Conclusion***

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.



If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

*Branda H/L*

BH

CHRISTOPHER REVAI  
PRIMARY EXAMINER

*CEL 3/26/06*